25 For 25
25 Things to Know/Try for a Better 2025

January 15, 2025

By Aaron Grothe
NEbraskaCERT

Introduction

25 for 25?

I did a 12 for 12 talk in 2012 and have just kept going from there. Used to say I was in a rut now describe it as a groove.

Links are at the end of the talk
Slides are posted at the NEbraskaCERT website
http://www.nebraskacert.org/csf

Introduction (Continued)

If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.

Introduction

Something New

Usually I put together the talk in August/September from notes earlier in the year and then continue to refine it until I give it in January. Replace a tip with a stronger one and so on.

This year I've saved a copy of my first complete set of 25 tips from September and have them at my website https://www.grothe.us

Currently it shares 16 of the 25 tips from this talk, combined a couple of them as well and added content to some others

Tip - Bindiff.

Bindiff is a very nice diff tool for showing the differences between disassembled code

It is being used by a lot of people along with Ghidra and/or IDA pro to reverse engineer patches that come out from Vendors

Used by VxSig to automatically generate AV byte signatures from similar binaries

Tip - Diffoscope.

Diffoscope is a tool that can tell you the differences between two things.

Potential use cases

- Want to know what changed in a ISO image between builds
- Differences between two folders of PDFs
- DIfferences between your incremental backups

Used by reproducible builds project

Tip - Reproducible Builds.

Reproducible builds are simply that you can compile a program and I can compile a program and get the same checksum.

The Debian, NixOS and Arch Linux projects are all working on this.

Reproducible builds will help make sure that nothing has changed in a program from what was generated by your vendor.

This is a big part of efforts to secure the Software Build of Materials (SBoM)

Tip - Safe C++/C

Memory Safety for C++???

Safe C++ is a working group going through C++ to work at creating a Memory Safe C++ variant.

Lot of production code is in C++ and if they can come up with a migration path. It might really help them out.

Groups such as the NSA have suggested migrating away from C++ to memory safe languages such as Rust.

Tip - Safe C++/C.

Memory Safety for C???

Fil-C and TrapC are both lightly modified versions of C designed to be memory safe.

Fil-C is modified to still have malloc calls, but has an internal garbage collector

TrapC gets rid of malloc replaces malloc with new, and uses its own garbage collection to handle freeing memory

Tip - arcX Cyber Threat Intelligence.

Cyber Threat Intelligence 101 Course is currently available for Free.

Is a good little certification you can get done in an afternoon.

Has a nice title and the training is pretty good.

Tip - Mullvad browser.

Mullvad is a company that offers a VPN solution. They've now created a browser.

Interesting concept they've taken the Tor Browser (based on Mozilla Firefox) and removed the Tor components.

Reduces the number of identifiable bits of data about your browser, according to the EFF's Panopticlick.

Also randomizes your HTML 5 Canvas, used by a lot of sites to uniquely identify you.

Tip - OneFileLinux.

OneFileLinux is a one file linux distribution that fits inside 20mb

Most UEFIs have 100mb of space and are usually half filled

You install this distribution into the EFI system partition and boot

- Doesn't appear in your filesystem
- Since the EFI partition isn't encrypted can theoretically be installed on systems with disk encryption turned on

Will leave the potential to install a covert operating system up to the user.

Tip - Datacenters Wasting Power.

Uptime institute estimates that if Datacenters started enabling powersaving settings in their servers they could reduce energy usage by up to 20-25% up to 50% in some cases

Drawback of this is that their would be a small pause for certain operations. E.g. severless operations would take a few more microseconds, etc.

Main change is modifying the processors to run in a higher P-state, e.g. P2 to reduce power usage

Less power usage, less cooling, less impact

Tip - Cosmospolitan/Llamafile.

Cosmopolitan - modifies the GCC and CLANG compilers to generate a single executable.

This executable will run natively on Linux, Mac, Windows, FreeBSD, OpenBSD, NetBSD, and BIOS for AMD64, and ARM64

Llamafile takes Cosmopolitan and combines it with an LLM into a single executable.

Great way to try out a LLM or create a pocketable AI demo

They have a handful of models ready to go.

Tip - LinuxServer.io

LinuxServer.io has docker images in their fleet for a lot of things

Some of the images available are

- Chromium
- Firefox
- Kali
- And about 1,000 more

If you want to run something in docker, it is a good place to look

Next slide shows how to run browser in a browser listening

Tip - LinuxServer.io.

Running docker firefox

```
Docker run -d \
 -name=firefox \
 -security-opt seccomp=unconfined `#optional` \
 -e PUID=1000 -e PGID=1000 \
 -e TZ=Etc/UTC \
 -e FIREFOX_CLI=https://www.linuxserver.io/ `#optional` \
 -p 3000:3000 -p 3001:3001 \
 -shm-size="1gb" \
 -restart unless-stopped \
 lscr.io/linuxserver/firefox:latest
```

Tip - Mandiant - North Korea Hackers.

Hackers from North Korea are applying for and getting IT remote working jobs in the US and England.

Sometimes they have an agent in the country who will host the laptop and help them appear to be in the US.

Goals for the North Koreans

- Hard currency
- Chance to infiltrate systems and put in long term backdoors
- Exfiltration of data for later blackmail

Tip - NIST - Post Quantum Standards.

Quantum computing is happening anytime between the next 5 and 50 years

There are reports that the Chinese and others are saving off large amounts of data for later decryption

NIST has approved three post encryption quantum standards

Tip - Dangerzone

Dangerzone

Takes potentially dangerous attachments in PDF, Microsoft Office, Libreoffice Document and image formats and converts them to safe pdfs

Uses two docker containers to do the conversion. So on Mac OS X and Microsoft windows works best with Docker desktop

Tip - Dangerzone.

How it works

First container opens the document using Libreoffice or PyMuPDF and converts it into RGB pixel data. Writes out data and quits

Second container reads the RGB pixel data and uses PyMuPDF to generate a searchable pdf file, that the user can then access

Not 100% certain to be safe, but defense in depth

Tip - PyPi Revival

How this one works

- Someone removes a package from the PyPi repository
  - Maintainer may have retired
  - Maintainer may have changed project name, etc.
- A hacker creates a new project with the same name
- People start downloading and getting hacked
- JFrog is reserving these packages to prevent that from happening

Tip - Extended Windows 10 Support.

Windows 10 goes End of Life October 25, 2025. Up until recently you had several options.

1. Upgrade to Windows 11 if you can/or force it to install on your PC - rufus, etc.
2. Upgrade to Linux :-)
3. Buy a new machine and turn your working PC into ewaste

Now there is a fourth option

Microsoft is offering an additional year of support for $30

Tip - Google Programmable Search Engine

Programmable Search Engine by Google allows you to create customized Programmable Search Engine

For example here is a google search engine that only searches the NEbraskaCERT CertConf site
https://www.certconf.org

<script async
src="https://cse.google.com/cse.js?cx=e011844ef84a54c77
">
</script>

Tip - Google Programmable Search Engine.

You can create these for sites you don't control. E.g. you need to do some recon on a site, create a custom search engine and you

Can create one that will search for only specific items, or sites. E.g. you can have it search for pdfs only on a site, or hit specific pages or specific topics

Allows you to bypass info you don't want and the AI summaries

Tip - Vulnhunter

Open Source tool designed to analyze Python code zero days

Looks for remote exploit vulnerabilities such as: SQL Injection, Arbitrary file overwrites, Cross-site scripting and others

Is currently going through 90 day disclosure for quite a few projects

Leverages the Claude AI currently, can be used with others

Assigns a score of 1 to 10 for vulnerability (7 is considered to probably be valid)

Tip - Vulnhunter.

Generates Proof of Concept (PoC) for vulnerability

Currently only does Python and requires static analyzers so can have larger number of false positives.

Interesting to see if this gets worked into CI/CD pipelines for OSS projects.

Keep in mind LLMs are not deterministic so you run it multiple times you'll probably get different results.

Tip - Raspberry PI Connect.

The Raspberry Pi guys are offering a new feature. You can use the Raspberry PI Connect software to connect to your Raspberry PI remotely.

The service is currently in beta and is free for one machine.

It allows you to connect to your desktop and command line via a web browser.

Requires a Raspberry Pi 4 or 5 though some people have gotten it to work on RPI3+, but that would be very slow.

Tip - AWS Kill Switch.

AWS Kill Switch is a project that can allow you to quickly lock down your AWS environment

Can lock down AWS Account and IAM roles during a security incident

E.g. you believe improper data has been uploaded to an S3 bucket. AWS Kill Switch, can pull all S3 access across your account while you figure things out.

Tip - Logging Made Easy

Logging Made Easy (LME) is a tool from CISA for Windows boxes that provides a simple log management system.

It isn't a SIEM. Could be quite useful for a SOHO environment

If you don't have a SOC, SIEM or another monitoring solution. LME can help provide you a basic level of auditing.

Tip - Logging Made Easy.

From their github page

- Show where administrative commands are being run on enrolled devices
- See who is using which machine
- In conjunction with threat reports, it is possible to query for the presence of an attacker in the form of Tactics, Techniques and Procedures (TTPs)

Still very early in development

Tip - Applicant Tracking System (ATS)

The Applicant Tracking System (ATS) score is a score generated by running your resume against a job opening.

If you don't get to a certain score (typically 80), you resume won't get to a human for review and will be automatically rejected.

There isn't a published algorithm for how to generate an ATS score (someone should write one).

There are services that will give you a limited number of ATS score evaluations, but they try and upsell you on this

Tip - Applicant Tracking System (ATS).

An example of a course correction on this

Half of Human resources were terminated at a tech company by the manager. After HR didn't forward a single application in 3 months

Managed then created a temporary email and submitted a carefully crafted resume that was rejected

ATS system was looking for AngularJS (a defunct technology) as opposed to Angular JS (which is very hot right now)

Tip - Sshamble.

Can identify misconfigurations in ssh settings.

Can also do some cool auditing things.

Scenario. Bill leaves the company

- Go through all the machines and see if there are any public keys that Bill could use to get back into a machine
- Can also be used to figure out other misconfigurations as well

Tip - LLMs hallucinating .

Large Language Models tend to hallucinate package names when you ask them to generate code for example.

E.g. it can tell you to import packages that don't exist

These names are generated in a semi-predictable way

Given that attackers can create these packages, insert malware and people will download them.

Largely an NPM/PyPi issue

Tip - Mystery Linux 9.9 CVE - its Cups

The week of September 23rd there was an announcement

A 9.9 CVE that is remotely exploitable and was in nearly every version of Linux will be receiving a patch

Given the overall description it sounded like the apocalypse. Assumptions ran wild. Would it be over something to do with SSH? Would it be related to some other utility that is accessible to most Linux systems connected to the internet.

Tip - Mystery Linux 9.9 CVE - its Cups.

Once it came out. The issue was with CUPs the printing system for Linux.

Most people don't have CUPs exposed to the internet so not quite the issue that it was described as.

That being said it was a 9.9 and if you had CUPS on your local network, most people do it was a heck of an attack vector.

Summary

Time to revisit my predictions for 2024.

- Cybersecurity is getting a higher profile in the government
  - Energy star system might be interesting
  - False Claims Act
- We're still using default passwords, and accounts in 2023/2024
- Licensing is going to be getting a lot more interesting in 2024
  - Companies are working to deal with hosting companies using their software
  - Companies are trying to make money on their software
- 2024 was an interesting year

Summary

So that was my 24 for 24's predictions. Time for my 2025 Predictions

- Cybersecurity positions will be augmented by AI more than ever before
  - Security Copilot from Microsoft is pretty interesting
  - AI LLMs are getting more and more powerful and cheaper for companies to implement their own private AI
- There will be a Cyber Attack / Ransomware attack that will have some loss of life (not one I'm thrilled with)
- 2025 is going to be another interesting year

Links

Tip - Bindiff

- https://www.helpnetsecurity.com/2023/09/25/bindiff-open-source-comparison-tool-for-binary-files/
- https://github.com/google/bindiff

Links

Tip - Diffoscope

- https://diffoscope.org/

Links

Tip - Reproducible Builds

- https://reproducible-builds.org/
- https://en.wikipedia.org/wiki/Reproducible_builds

Links

Tip - Safe C++

- https://www.theregister.com/2024/09/16/safe_c_plusplus/
- https://safecpp.org/P3390R0.html

Links

Tip - Fil-C

- https://www.theregister.com/2024/11/16/rusthaters_unite_filc/?td=rt-3a
- https://github.com/pizlonator/llvm-project-deluge/blob/deluge/Manifesto.md

TIp - TrapC

- https://www.theregister.com/2024/11/12/trapc_memory_safe_fork/
- https://vimeo.com/1028578347

Links

Tip - arcX Cyber Threat Intelligence

- https://arcx.io/courses/cyber-threat-intelligence-101

Links

Tip - Mullvad Browser

- https://mullvad.net/en/download/browser/linux
- https://news.ycombinator.com/item?id=37159744
- https://github.com/mullvad/mullvad-browser?tab=readme-ov-file

Links

Tip - OneFileLinux

- https://github.com/zhovner/OneFileLinux
- https://www.theregister.com/2024/09/09/onefilelinux_esp_distro/

Links

Tip - Data Center Power waste

- https://www.theregister.com/2024/09/20/datacenters_waste_watts_server_power/
- https://journal.uptimeinstitute.com/managing-server-performance-for-power-a-missed-opportunity/

Links

Tip - Cosmopolitan

- https://github.com/jart/cosmopolitan

Tip - Llamafile

- https://github.com/Mozilla-Ocho/llamafile
- https://future.mozilla.org/builders/news_insights/introducing-llamafile/

Links

Tip - LinuxServer.io

- https://www.linuxserver.io/
- https://fleet.linuxserver.io/
- https://www.youtube.com/watch?v=RUqGlWr5LBA

Links

Tip - Mandiant - North Korea Hackers

- https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat/
- https://www.theregister.com/2024/09/24/mandiant_north_korea_workers/
- https://www.theregister.com/2024/10/18/ransom_fake_it_worker_scam/

Links

Tip - DangerZone

- https://dangerzone.rocks/
- https://gijn.org/stories/cutting-edge-free-online-investigative-tools/

Links

Tip - NIST - approves post quantum encryption standards

- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Links

Tip - PyPi Revival

- https://jfrog.com/blog/revival-hijack-pypi-hijack-technique-exploited-22k-packages-at-risk/

Links

Tip - Extended Windows 10 Support

- https://www.theverge.com/2024/10/31/24284398/microsoft-windows-10-extended-security-updates-consumer-pricing
- https://www.tomshardware.com/software/operating-systems/microsoft-will-charge-windows-10-users-usd30-per-year-for-security-updates

Links

Tip - Google Programmable Search Engine

- https://programmablesearchengine.google.com/about/
- https://lifehacker.com/tech/use-programmable-search-engine-to-build-a-cleaner-version-of-google

Links

Tip - Vulnhunter

- https://github.com/protectai/vulnhuntr
- https://www.theregister.com/2024/10/20/python_zero_day_tool/
- https://huntr.com/

Tip - Naptime (Google Project)

- https://googleprojectzero.blogspot.com/2024/06/project-naptime.html

Links

Tip - Raspberry PI Connect

- https://www.raspberrypi.com/software/connect/

Links

Tip - AWS Kill Switch

- https://www.helpnetsecurity.com/2023/11/27/aws-kill-switch-open-source-incident-response-tool/
- https://github.com/secengjeff/awskillswitch

Links

Tip - Logging Made Easy

- https://www.helpnetsecurity.com/2023/10/30/logging-made-easy-lme-free-log-management/
- https://github.com/cisagov/LME

Links

Tip - Application Tracking System (ATS)

- https://timesofindia.indiatimes.com/technology/social/why-this-us-based-it-company-fired-its-entire-hr-team/articleshow/113833438.cms
- https://www.msn.com/en-in/news/other/from-hiring-to-firing-entire-hr-team-terminated-after-manager-s-own-resume-fails-automated-screening/ar-AA1rspFK

Links

Tip - Sshamble

- https://www.helpnetsecurity.com/2024/08/08/sshamble-test-ssh-services/
- https://github.com/runZeroInc/sshamble
- https://www.runzero.com/sshamble/

Links

Tip - LLMs hallucinating Package names

- https://www.theregister.com/2024/09/30/ai_code_helpers_invent_packages/
- https://www.theregister.com/2024/03/28/ai_bots_hallucinate_software_packages/
- https://arxiv.org/abs/2406.10279

Links

Tip - Mystery Linux 9.9 CVE - its Cups

- https://www.theregister.com/2024/09/26/cups_linux_rce_disclosed/
- https://securityintelligence.com/news/fysa-critical-rce-flaw-in-gnu-linux-systems/